09/910,416

IN THE CLAIMS

Please amend claims 1, 2, 3, 4, 7, 8, 9, 10, 11, 13 and 14; cancel claims 12 and 15 and add new claims 16-19 as follows:

1.   (Currently Amended) A secure transport system for transporting secure packets from a first node to a second node, comprising:

a first node that creates secure packets, wherein each secure packet contains identical retrieval information;

[a first] multiple secure relays that receive[s] secure packets and non secure packets from multiple nodes or other secure relays, wherein said multiple secure relays are capable of identifying retrieval information in each secure packet, wherein [the] each of said multiple secure relays forwards [each] secure packets to another of said multiple [different] secure relays and forwards non-secure packets to destination relays, and wherein [the] said multiple secure relays forward[s each] secure packets to the second node when a retrieval condition has been indicated, and wherein each of said multiple secure relays forwards secure packets to another of said multiple secure relays when the retrieval condition has not been indicated; and

a second node that creates a [relay] retrieval condition related to said retrieval information in said multiple secure packets and receives the secure packets, wherein said first or second nodes are not associated with said multiple secure relays.

2.   (Currently Amended)   A method for transmitting packets in a secure format from a first node to a second node, comprising the steps, executed in a data processing system, of:

receiving secure packets in a first secure relay or a second secure relay from the first node, wherein said secure packets contain retrieval information based on information provided by the first node;

determining if a retrieval condition has been indicated by identifying said secure packets that contain the same retrieval information based on information provided by the second node;

forwarding all secure packets associated with the retrieval condition to the second node if the retrieval condition has been indicated, wherein said second node may be the first node; and

-2-

09/910,416

forwarding all [the] secure packets to another secure relay if the retrieval condition has not been indicated.

3.   (Currently Amended)   The method of claim 2, further comprising:

creating secure packets in a first node, wherein said secure packets contain identical retrieval information; [and]

transmitting the secure packets to random secure relays, wherein the random secure relays include the first secure relay and the second secure relay; and

providing a unique identifying flag from the second node to the fist and second secure relays, wherein said unique identifying flag identifies secure packets that contain the same retrieval information.

4.   (Currently Amended)   The method of claim 2, wherein determining if a retrieval condition has been indicated further comprises:

receiving a retrieval packet from the second node in the first and second secure relays that indicates the retrieval condition for secure packets, wherein said retrieval packet contains a flag that instructs said first and second secure relays to identify secure packets that contain the same retrieval information; and

forwarding any secure packet from said first and second secure relays associated with the retrieval packet to the second node once the retrieval packet has been received.

5.   (Original)   The method of claim 4, further comprising: determining if a secure packet is associated with the retrieval packet by using a key algorithm.

6.   (Original)   The method of claim 2, wherein forwarding the secure packet to the second node further comprises forwarding secure packets associated with the retrieval condition to the second node.

7.   (Currently Amended)   The method of claim 2, wherein forwarding the secure packets to another secure relay further comprises:

-3-

09/910,416

randomly selecting [a second] other secure relays to forward a secure packet to, wherein said secure packets are in transition and not discoverable until a retrieval condition has been indicated; and

modifying a header associated with each secure packet to reflect the [second] other secure relay.

8.   (Currently Amended) A method for maintaining a secure distributed storage system by initiating a [transmitting] transmission of a message from a first node to a second node in a secure manner, wherein the second node may be the first node, comprising the steps, executed in a data processing system, of:

creating a set of secure packets associated with the message, wherein each secure packet[s have and associated] contains an identical first retrieval key, wherein the first retrieval key is created by the first node;

forwarding the set of secure packets to multiple secure relays from the first node;

forwarding the set of secure packets [to between] among secure [routers] relays so long as a second retrieval key associated with the first retrieval key is not received in the said multiple secure relays, wherein said second retrieval key is created by the first or second node; and

forwarding the set of secure packets to the second node once the second retrieval key is received in the said multiple secure relays.

9.   (Currently Amended)   The method of claim 8, further comprising:

creating a second retrieval key in a second node, wherein said second retrieval key is associated with destination information for the set of secure packets and information for identification of said first retrieval key;

transmitting [a] said second retrieval key from the second node to said multiple [a] secure [routers] relays.[; and

[forwarding the retrieval key to multiple secure routers.]

10.   (Currently Amended)   [A] The method of claim 8 [for receiving a message at a node, wherein the message contains multiple secure packets], further comprising the steps of:

- 4 -

09/910,416

[transmitting a retrieval key to a secure router from the node, wherein the retrieval key is associated with the multiple secure packets;

receiving from a secure router secure packets associated with the retrieval key;]

at the second node, resequencing the set of secure packets to recreate the message based on resequencing information associated with the set of secure packets .

11. (Currently Amended) The method of claim 10, further comprising the steps of:

at the second node, creating a second retrieval key based on the location of the second node [message], wherein said second retrieval key is created based on the following methods:

[This retrieval key could be triggered any number of methods (ex. 1.] automatically using a built in time delay created during the creation of the secure packets of data, [2.] by a client transmitting a retrieval key to relays, or [3.] some other event, such as data integrity check, network outage or insufficient client funds]D].

12. (Canceled)

13. (Currently Amended) The method of claim [12] 2, wherein forwarding [the] all secure packets to another [from one] secure relay [to another secure relay] further comprises the steps of:

at the forwarding secure relay, replacing a destination header in [a] all secure packets with a random secure relay; and

at the forwarding secure relay, replacing a destination header in [a] all secure packets with the [destination] second node when the retrieval condition has been indicated [key is received].

14. (Currently Amended) [A] The method of claim 2, further comprising:

[billing for the secure transport service compromising:]

[creation of] creating secure packets [could], wherein said secure packets in said first node require a fee to ["enter" the network of] be transmitted to said first and second secure relays;

- 5 -

creating a retrieval condition, wherein said retrieval condition initiates forwarding of said secure packets to said second node;

generating a billing event and wherein said billing event is based on parameters, such as time size, source destination, encryption level, iterations of data.

[creation of a retrieval key could trigger a billing (ex. Invoice generated or charge a credit card) by the service provider/communications carrier, perhaps based on any one or many parameters (time, size, source, destination, tariffs, encryption level, iterations of data).]

15. (Canceled)

16. (New)   The system of claim 1, wherein the second node creates a retrieval condition by generating a unique identifying flag that identifies said multiple secure packets that contain the same retrieval information, and wherein said second node transmits said identifying flag to said multiple secure relays to initiate transmission of said multiple secure packets to said second node, and wherein said first or second nodes may create said retrieval condition.

17. (New) The system of claim 1, wherein the second node successively forwards multiple identical retrieval packets to said multiple secure relays, wherein each retrieval packet indicates the retrieval condition for secure packets and wherein each said retrieval packet contains a flag that instructs said multiple secure relays to identify secure packets that contain the same retrieval information.

18. (New) The method of claim 2, further comprising the steps of:

forwarding all secure packets to a non secure relay, wherein said non secure relay forwards said secure packet to other secure relays based on a table.

19. (New) The method of claim 2, wherein determining if a retrieval condition has been indicated further comprises the steps of:

at the first or second node, successively forwarding multiple identical retrieval packets to the first and second secure relays, wherein each retrieval packet indicates the

- 6 -

09/910,416

retrieval condition for secure packets and wherein said retrieval packet contains a flag that instructs said first and second secure relays to identify secure packets that contain the same retrieval information.

-7-